AMENDMENTS TO THE CLAIMS

1.   (Currently Amended) A method of comparing access control lists to configure a security policy on a network, the method comprising the computer-implemented steps of:

identifying ~~one or more~~ first sub-entries in a first access control list;

identifying ~~one or more~~ second sub-entries in a second access control list;

programmatically determining whether a first access control list is functionally equivalent to a second access control list in order to configure the security policy on the network by determining whether each first sub-entry <u>in the first access control list</u> is equivalent to ~~one or more~~ <u>at least one</u> of the second sub-entries; and

determining that the first access control <u>list</u> is functionally equivalent to the second access control list only when each of the first sub-entries is equivalent to ~~one or more~~ <u>at least one</u> of the second sub-entries.

2.   (Currently Amended) A method as recited in Claim 1, wherein programmatically determining whether a first access control list is equivalent to a second access control list includes:

identifying a dimensional range for each policy action specified in the first access control list, the dimensional range of each policy action characterizing communication packets specified by ~~one or more~~ entries in the first access control list for that ~~that~~ policy action;

identifying a dimensional range for each policy action specified in the second access control list, the dimensional range of each policy action characterizing communication packets specified by ~~one or more~~ entries in the second access control list for that ~~that~~ policy action; and

determining whether the dimensional range identified for each policy action in the first access control list is equivalent to the dimensional range identified for each policy action in the second access control list.

3.   (Original) A method as recited in Claim 2, wherein identifying a dimensional range for each policy action specified in the first access control list and in the second access control list includes identifying a source address range and a destination address range for

4   communication packets specified by each of the entries in the first access control list and in

5   the second access control list.

1   4.   (Original) A method as recited in Claim 2, wherein identifying a dimensional range

2   for each policy action specified in the first access control list and in the second access control

3   list includes identifying a source port range and a destination port range for communication

4   packets specified by each of the entries in the first access control list and in the second access

5   control list.

1   5.   (Original) A method as recited in Claim 2, wherein identifying a dimensional range

2   for each policy action specified in the first access control list and in the second access control

3   list includes identifying a communication protocol for communication packets specified by

4   each of the entries in the first access control list and in the second access control list.

1   6.   (Currently Amended) A method as recited in Claim 1, wherein the first access

2   control list and the second access control list each specify a plurality of entries, and each

3   entry identifies a dimensional range for a policy action, the dimensional range characterizing

4   communication packets that are to be affected by the policy action, and wherein

5   programmatically determining whether a first access control list is equivalent to the second

6   access control list includes:

7   determining whether each entry in the first access control list has a dimensional range

8   that is either equivalent to or contained by the dimensional range of ~~one or~~

9   ~~more~~ entries in the second access control list that specify the policy action of

10   the entry in the first access control list.

1   7.   (Currently Amended) A method as recited in Claim 1, wherein the first access

2   control list and the second access control list each specify a plurality of entries, and each

3   entry identifies a dimensional range for a policy action, the dimensional range characterizing

4   communication packets that are to be affected by the policy action, and wherein

5   programmatically determining whether a first access control list is equivalent to the second

6   access control list includes:

7   determining whether each entry in the first access control list has a dimensional range

8   that is either equivalent to or contained by the dimensional range of ~~one or~~

9   ~~more~~ entries in the second access control list that specify the policy action of

10   the entry in the first access control list; and

11 determining whether each entry in the second access control list has a dimensional

12   range that is either equivalent to or contained by the dimensional range of ~~one~~

13   ~~or more~~ entries in the first access control list that specify the same policy

14   action.

1   8.   (Canceled)

1   9.   (Currently Amended) A method of comparing access control lists to configure a

2   security policy on a network, the method comprising:

3   identifying a dimensional range and a policy action for each entry in a first access

4   control <u>list</u>;

5   identifying all overlapping dimensional ranges in the first access control list, each

6   overlapping dimensional range corresponding to where the dimensional

7   ranges of ~~two or more~~ entries in the first access control list overlap;

8   identifying all non-overlapping dimensional ranges in the first access control list,

9   each of the non-overlapping dimensional ranges corresponding to dimensional

10   ranges of entries in the first access control list that do not overlap dimensional

11   ranges of other entries in the first access control list;

12   identifying a policy action for each identified overlapping dimensional range of the

13   first access control list;

14   identifying a policy action for each identified non-overlapping dimensional range of

15   the first access control list; and

16   determining whether each identified overlapping and non-overlapping dimensional

17   range identified from the first access control list is contained by or equal to a

18   dimensional range of ~~one or more~~ entries in a second access control list in

19   which the ~~one or more~~ entries of the second access control list have the policy

20   action of that identified overlapping or non-overlapping dimensional range<u>;</u>

21   <u>wherein identifying a policy action for each identified overlapping dimensional range</u>

22   <u>of the first access control list includes using a conflict rule to determine the</u>

23   <u>policy action from a first policy action of a first entry having a dimensional</u>

24   <u>range within the overlapping dimensional range, and from a second policy</u>

25   <u>action of a second entry having a dimensional range within the overlapping</u>

26   <u>dimensional range, wherein the second policy conflicts with the first policy.</u>

1   10.   (Currently Amended) A method as recited in Claim 9, further comprising:

2   identifying a dimensional range and a policy action for each entry in the second

3   access control;

4   identifying all overlapping dimensional ranges in the second access control list, each

5   overlapping dimensional range corresponding to where the dimensional

6   ranges of ~~two or more~~ entries in the second access control list overlap;

7   identifying all non-overlapping dimensional ranges in the second access control list,

8   each of the non-overlapping dimensional ranges corresponding to dimensional

9   ranges of entries in the second access control list that do not overlap

10   dimensional ranges of other entries in the second access control list;

11   identifying a policy action for each identified overlapping dimensional range in the

12   second access control list;

13   identifying a policy action for each identified non-overlapping dimensional range of

14   the second access control list; and

15   determining whether each identified overlapping and non-overlapping dimensional

16   range identified from the second access control list is contained by or equal to

17   a dimensional range of ~~one or more~~ entries in the first access control list in

18   which the ~~one or more~~ entries of the first access control list have the policy

19   action of that identified overlapping or non-overlapping dimensional range.

1   11.   (Currently Amended) A method as recited in Claim 9, wherein:

2   identifying a dimensional range and a policy action for each entry in the second

3   access control list;

4   identifying all overlapping dimensional ranges in the second access control list, each

5   overlapping dimensional range corresponding to where the dimensional

6   ranges of ~~two or more~~ entries in the second access control list overlap;

7   identifying all non-overlapping dimensional ranges in the second access control list,

8   each of the non-overlapping dimensional ranges corresponding to dimensional

9	ranges of entries in the second access control list that do not overlap
10	dimensional ranges of other entries in the second access control list;
11	identifying a policy action for each identified overlapping dimensional range of the
12	second access control list;
13	identifying a policy action for each identified non-overlapping dimensional range of
14	the second access control list; and
15	~~and~~ wherein determining whether each identified overlapping and non-overlapping
16	dimensional range of the first access control list is contained by or equal to a
17	dimensional range of ~~one or more~~ entries in a second access control list
18	includes determining whether each identified overlapping and non-
19	overlapping dimensional range identified from the first access control list is
20	contained by or equal to ~~one or more~~ overlapping and non-overlapping
21	dimensional ranges of the second access control list.

1   12.   (Canceled)

1   13.   (Currently Amended) A method as recited in Claim [[12]]9, wherein using a conflict
2   rule to determine the policy action <u>comprises</u> selecting one of the first policy or the second
3   policy based on the selected first or second policy being newer.

1   14.   (Original) A method as recited in Claim 9, wherein identifying a dimensional range
2   and a policy action for each entry in the first access control list includes identifying a source
3   address range and a destination address range for communication packets specified by each
4   of the entries in the first access control list.

1   15.   (Original) A method as recited in Claim 9, wherein identifying a dimensional range
2   and a policy action for each entry in the first access control list includes identifying a source
3   port range and a destination port range for communication packets specified by each of the
4   entries in the first access control list.

1   16.   (Original) A method as recited in Claim 9, wherein identifying a dimensional range
2   and a policy action for each entry in the first access control list includes identifying a

3   communication protocol for communication packets specified by each of the entries in the

4   first access control list.

1   17.   (Currently Amended) A computer readable medium for comparing access control

2   lists to configure a security policy on a network, the computer readable medium carrying

3   instructions for performing the steps of:

4   identifying ~~one or more~~ first sub-entries in a first access control list;

5   identifying ~~one or more~~ second sub-entries in a second access control list;

6   programmatically determining whether a first access control list is functionally

7   equivalent to a second access control list in order to configure the security

8   policy on the network by determining whether each first sub-entry is

9   equivalent to ~~one or more~~ at least one of the second sub-entries; and

10   determining that the first access control list is functionally equivalent to the second

11   access control list only when each of the first sub-entries is equivalent to ~~one~~

12   ~~or more~~ at least one of the second sub-entries.

1   18.   (Currently Amended) A computer readable medium as recited in Claim 17, wherein

2   instructions for programmatically determining whether a first access control list is equivalent

3   to a second access control list include instructions for:

4   identifying a dimensional range for each policy action specified in the first access

5   control list, the dimensional range of each policy action characterizing

6   communication packets specified by ~~one or more~~ entries in the first access

7   control list for that that policy action;

8   identifying a dimensional range for each policy action specified in the second access

9   control list, the dimensional range of each policy action characterizing

10   communication packets specified by ~~one or more~~ entries in the second access

11   control list for that that policy action; and

12   determining whether the dimensional range identified for each policy action in the

13   first access control list is equivalent to the dimensional range identified for

14   each policy action in the second access control list.

1   19.   (Original) A computer readable medium as recited in Claim 17, wherein instructions

2   for identifying a dimensional range for each policy action specified in the first access control

3 list and in the second access control list include instructions for identifying a source address

4 range and a destination address range for communication packets specified by each of the

5 entries in the first access control list and in the second access control list.

1 20. (Original) A computer readable medium as recited in Claim 19, wherein instructions

2 for identifying a dimensional range for each policy action specified in the first access control

3 list and in the second access control list include instructions for identifying a source port

4 range and a destination port range for communication packets specified by each of the entries

5 in the first access control list and in the second access control list.

1 21. (Original) A computer-readable medium as recited in Claim 17, wherein instructions

2 for identifying a dimensional range for each policy action specified in the first access control

3 list and in the second access control list include instructions for identifying a communication

4 protocol for communication packets specified by each of the entries in the first access control

5 list and in the second access control list.

1 22. (Currently Amended) A computer-readable medium as recited in Claim 17, wherein

2 the first access control list and the second access control list each specify a plurality of

3 entries, and each entry identifies a dimensional range for a policy action, the dimensional

4 range characterizing communication packets that are to be affected by the policy action, and

5 wherein instructions for programmatically determining whether a first access control list is

6 equivalent to the second access control list includes instructions for determining whether

7 each entry in the first access control list has a dimensional range that is either equivalent to or

8 contained by the dimensional range of ~~one or more~~ entries in the second access control list

9 that specify the same policy action.

1 23. (Currently Amended) A computer-readable medium as recited in Claim 17, wherein

2 the first access control list and the second access control list each specify a plurality of

3 entries, and each entry identifies a dimensional range for a policy action, the dimensional

4 range characterizing communication packets that are to be affected by the policy action, and

5 wherein instructions for programmatically determining whether a first access control list is

6 equivalent to the second access control list includes instructions for:

7	determining whether each entry in the first access control list has a dimensional range
8	that is either equivalent to or contained by the dimensional range of ~~one or~~
9	~~more~~ entries in the second access control list that specify the same policy
10	action; and
11	determining whether each entry in the second access control list has a dimensional
12	range that is either equivalent to or contained by the dimensional range of ~~one~~
13	~~or more~~ entries in the first access control list that specify the same policy
14	action.

1	24.	(Canceled)

1	25.	(Currently Amended) A computer system for comparing access control lists to
2		configure a security policy on a network, the computer system comprising:
3		means for identifying ~~one or more~~ first sub-entries in a first access control list;
4		means for identifying ~~one or more~~ second sub-entries in a second access control list;
5		means for programmatically determining whether a first access control list is
6		functionally equivalent to a second access control list in order to configure the
7		security policy on the network by determining whether each first sub-entry is
8		equivalent to ~~one or more~~ at least one of the second sub-entries; and
9		means for determining that the first access control <u>list</u> is functionally equivalent to the
10		second access control list only when each of the first sub-entries is
11		equivalent to ~~one or more~~ at least one of the second sub-entries.

1	26.	(Currently Amended) A policy server communicatively coupled to ~~one or more~~
2		security devices in a network to configure a security policy on a network, the policy server
3		comprising:
4		a processor;
5		a network interface that communicatively couples the processor to the network to
6		receive ~~one or more~~ flows of packets therefrom;
7		a memory; and
8		~~one or more~~ sequences of instructions in the memory which, when executed by the
9		processor, cause the processor to carry out the steps of:
10		identifying ~~one or more~~ first sub-entries in a first access control list;

11	identifying ~~one or more~~ second sub-entries in a second access control list;
12	programmatically determining whether a first access control list is functionally
13	equivalent to a second access control list in order to configure the security
14	policy on the network by determining whether each first sub-entry is
15	equivalent to ~~one or more~~ at least one of the second sub-entries; and
16	determining that the first access control is functionally equivalent to the second
17	access control list only when each of the first sub-entries is equivalent to ~~one~~
18	~~or more~~ at least one of the second sub-entries.

1	27.	(Original) The policy server of claim 26, wherein further comprising a memory to
2		store a plurality of access control lists, including the first access control list and the second
3		access control list, and wherein the processor is configured to configure each security device
4		on the network with at least one of the plurality of access control lists.

1	28.	(Currently Amended) The policy server of claim 26, wherein the processor is
2		configured to:
3		identify a dimensional range for each policy action specified in the first access control
4		list, the dimensional range of each policy action characterizing
5		communication packets specified by ~~one or more~~ entries in the first access
6		control list for that that policy action;
7		identify a dimensional range for each policy action specified in the second access
8		control list, the dimensional range of each policy action characterizing
9		communication packets specified by ~~one or more~~ entries in the second access
10		control list for that that policy action; and
11		determine whether the dimensional range identified for each policy action in the first
12		access control list is equivalent to the dimensional range identified for each
13		policy action in the second access control list.